REMARKS

In reply to the Office Action of October 22, 2003, Applicant submits the following remarks. Claims 1-9 have been amended. Claims 10-29 have been added. No new matter has been added. Claims 1-29 are now pending after entry of this amendment. Applicant respectfully requests reconsideration in view of the foregoing amendments and these remarks.

Section 102 Rejections

Claims 1-9 were rejected under 35 U.S.C. 102(e) as allegedly being anticipated by U.S. Patent Number 6,549,626 ("Al-Salqan"). Applicant respectfully traverses.

Amended claim 1 recites a method for transmitting a message from a sender to an intended recipient. The method includes encrypting a message using a symmetric key and sending the encrypted message to an intended recipient without making the symmetric key immediately accessible to the recipient. The symmetric key is provided to a third party. If the intended recipient signs and returns to the third party a receipt for the message, the receipt is transferred to the sender by the third party and the symmetric key is provided to the intended recipient.

Al-Salqan recites a method for encoding keys for storage, where the key is a private key or key password, such that the key can be decrypted if the key is lost or unavailable (Abstract, lines 1-3). A principal's private information, such as the principal's mother's maiden name or social security number, is encoded (column 2, lines 50-52). The encoded result is used to symmetrically encrypt the private key or password (column 2, lines 52-54). The private key or password is again encrypted using the public key of a trusted party, such as a certification authority (column 2, lines 54-57). The result of the two encryptions is a key recovery file that may be stored by the principal or other trusted party (column 2, lines 57-59). When the private key is lost or unavailable, the stored key recovery file can be accessed and decrypted (column 2, lines 59-63). The principal, or another party available to provide the principal's private information, can retrieve the key recovery file and key (column 7, lines 21-26).

Al-Salqan teaches a method where a key recovery file is stored such that the key recovery file and key can be accessed by a principal or a party who has access to the principal's private information, i.e., the information that was encoded and used to symmetrically encrypt the principal's private key or password. Al-Salqan's method of encoding keys for storage does not include encrypting a message with a symmetric key, sending the encrypted message to an intended recipient and sending the symmetric key to a third party. Rather, in the key recovery file method Al-Salqan teaches encrypting a private key or password and sending the encrypted key or password to a third party, but Al-Salqan does not teach or suggest sending a message encrypted with the key sent to the third party to an intended recipient. Because there is no message encrypted with a key that is sent to a third party, Al-Salqan does not teach or suggest generating a receipt for an encrypted message where the receipt is transferred by a recipient to a third party. It therefore follows that the symmetric key cannot be provided to the intended recipient upon a receipt for the message being transferred to a third party. Because Al-Salqan does not teach or suggest a recipient providing a receipt for a message encrypted by a key sent to a third party, Al-Salqan does not suggest or disclose encrypting a message with a symmetric key, sending the encrypted message to an intended recipient without making the symmetric key immediately accessible to the intended recipient, providing the symmetric key to a third party and providing the symmetric key to the intended recipient of the message if the intended recipient signs and returns a receipt for the message to the third party.

Al-Salqan also describes two different types of conventional encryption for maintaining information security, symmetrical encryption and asymmetric encryption (column 1, lines 21-60). Symmetric encryption uses the same key to encrypt and decrypt information and can be used when transmitting a message from a sender to a recipient as long as the two have agreed upon the key (*id.*). Asymmetric encryption uses a public key for encryption and a separate, mathematically related private key for decryption (*id.*). The principal shares the public key with those the principal expects will send him or her encrypted messages while maintaining the secrecy of the private key (*id.*). A trusted party, known as a certificate authority, can issue a

certificate that binds the public key and identity of the principal so that third parties can verify the identity of the principal (*id.*).

Applicant's claimed invention as recited in claim 1 uses a symmetric key for encrypting a message. The encrypted message is sent to an intended recipient without making the key immediately available to the recipient. Al-Salqan actually teaches away from claim 1. Al-Salqan states that symmetric key encryption can be used "as long as the sender and the recipient have agreed upon the key". Claim 1 requires that the key is not immediately available to the recipient and thus the method can be used even when the intended recipient and sender have had no previous communications or interactions.

Further, in Al-Salqan's description of a symmetric encryption method, only two parties are involved, a sender and a recipient. Applicant's claimed invention as recited in claim 1 requires a sender, a recipient and a third party. Thus, Al-Salqan does not suggest or disclose a method including sending an encrypted message to an intended recipient without making the encrypting key immediately accessible to the recipient, providing the key to a third party and sending the key to the recipient if the recipient signs and returns to the third party a receipt for the message.

The Examiner correlates a certificate to Applicant's receipt for a message. Al-Salqan teaches an asymmetric key encryption method that includes a certificate authority issuing a certificate so that third parties can verify the identity of a principal. Applicant points out that the certificate allows a third party to verify the identity of a principal by binding a public key, or asymmetric key, with the principal. Unlike a certificate, Applicant's receipt verifies receipt of a message. A certificate verifying the identity of a principal is not a receipt for a message.

Al-Salqan does not suggest or disclose encrypting a message with a symmetric key and sending the message to an intended recipient without making the symmetric key immediately accessible to the recipient. Further, Al-Salqan does not suggest or disclose the steps of providing a symmetric key to a third party and providing the symmetric key to the intended recipient if the intended recipient signs and returns a receipt for a message to the third party. For at least the

foregoing reasons, Applicant submits that claim 1 and its dependent claim 2 are not anticipated by Al-Salqan.

Amended claim 3 recites a method of message transmission from a sender to an intended recipient. At the sender, a message is encrypted using a symmetric key and the symmetric key is encrypted to make the symmetric key accessible to a third party but not immediately accessible to the recipient. The encrypted message and the encrypted symmetric key are sent to the intended recipient. At the recipient, a receipt for the message is signed and the receipt and the encrypted symmetric key are sent to the third party. At the third party, the receipt is transferred to the sender and the symmetric key is provided to the intended recipient if the receipt is properly signed.

As stated above, Al-Salqan teaches a certificate, but does not suggest or disclose a receipt for a message. It follows that Al-Salqan therefore does not suggest or disclose a method where at a recipient, a receipt for a message is signed and sent along with an encrypted symmetric key to a third party. Further, Al-Salqan does not suggest or disclose a method where at a third party, a receipt is transferred to a sender and a symmetric key is provided to an intended recipient if the receipt is properly signed. For at least these reasons, Applicant submits that claim 3 is not anticipated by Al-Salqan.

Amended claim 4 recites a method for certifying receipt of a message sent from a sender to an intended recipient, wherein the method is executed at a third party that is distinct from a sender and a receiver. The method includes receiving a signed receipt that memorializes receipt of an encrypted message and an encrypted key from an intended recipient, verifying the signed receipt, transferring the verified receipt and providing a symmetric key.

Although Al-Salqan teaches a certificate that is issued by a certificate authority and a key recovery file, neither of these is a receipt. Al-Salqan does not suggest or disclose a third party receiving a signed receipt memorializing receipt of an encrypted message, verifying the signed receipt and providing a symmetric key. For at least this reason, claim 4 is not anticipated by Al-Salqan.

Amended claim 5 recites a method for certifying receipt of a message sent from a sender to an intended recipient, wherein the method is executed at a third party distinct from a sender and a receiver. The method includes receiving a certified receipt from an intended receiver where the certified receipt includes a message identifier signed by the recipient and verifying the certified receipt. Again, Al-Salqan does not suggest or disclose receiving a receipt including a message identifier signed by the recipient or verifying a receipt.

Amended claim 6 recites a method including receiving from a third party a certified receipt that is verified by the third party and indicates that an intended recipient received a message where the message was encrypted using a symmetric key.

Al-Salqan does not disclose or suggest receiving a certified receipt from and verified by a third party, where the receipt indicates that an intended recipient receives a message that was encrypted using a symmetric key. For at least this reason, Applicant submits that claim 6 is allowable over Al-Salqan.

Amended claim 7 recites a method including creating a message header that includes a symmetric key and a message identifier associated with a message, encrypting the message with the symmetric key, encrypting the message header with a public key of a third party and attaching the message header to the encrypted message forming a certified message that is forwarded to an intended recipient. A certified receipt from the intended recipient that has been verified at the recipient is received and forwarded to a sender after verification. The validity of the receipt is verified using the stored symmetric key and the certified message.

Al-Salqan does not disclose or suggest at least the step of receiving a certified receipt originating from an intended recipient, where the certified receipt is verified at a third party and forwarded to a sender after verification. For at least this reason, claim 7 is not anticipated by Al-Salqan.

Claim 8 recites a method for providing a receipt for a message including creating a receipt for an encrypted message, including signing a hash of an encrypted message and returning the signed receipt to a third party. After verification of the signed receipt at the third party, the symmetric key is received from the third party.

As stated above, Al-Salqan recites a certificate authority that can issue a certificate linking a principal to a public key. However, issuing a certificate does not include providing a receipt for an encrypted message that includes a signed hash of the encrypted message, returning the signed receipt to a third party and receiving a symmetric key from the third party after verification of the signed receipt. For at least this reason, Applicant submits that claim 8 is not anticipated by Al-Salqan. Claim 9 depends from claim 8 and is similarly not anticipated.

Section 101 Rejections

Claims 1-9 were rejected based on 35 U.S.C. § 101 because they were directed to non-statutory subject matter. Applicant respectfully traverses. While Applicant disagrees with the Examiner's rejection, Applicant has amended each of the originally proposed claims to indicate the claimed methods are in fact computer-implemented methods. Applicant respectfully asserts the claims as amended are directed to statutory subject matter.

Enclosed is a $296 check for excess claim fees. Please apply any other appropriate charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 22 January 2004

Jennifer A. Zamorco
Reg. No. 54,563

Fish & Richardson P.C.
500 Arguello Street, Suite 500
Redwood City, California 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071